SAFETY MANUAL

SIL 2 Bus-Powered Digital Output Driver
DIN-Rail
Model D5240T

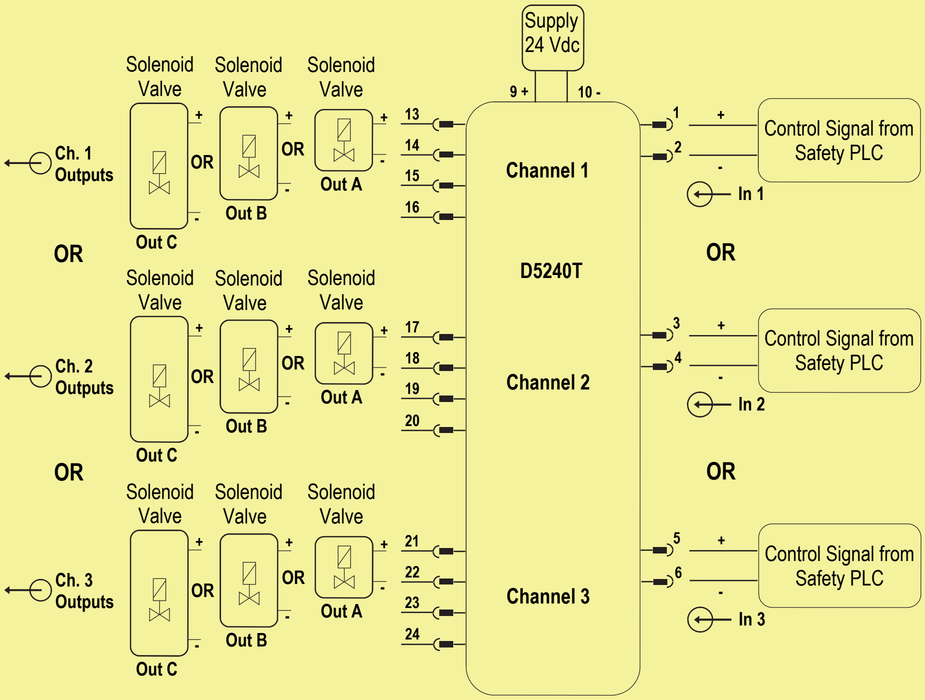
Approval:

SIL 3 Functional Safety TÜV Certificate conforms to IEC61508:2010 Ed.2, for Management of Functional Safety.

Reference must be made to the relevant sections within the instruction manual ISM0209 and ISM0154 (for SWC5090 Configuration Software instruction manual), which contain basic guides for the installation and configuration of the equipment.

gmi technology for safety

1st application of D5240T, with only an input channel (1 or 2 or 3) and one of three (A or B or C) its outputs for NE load



For each input signal:
0 Vdc ≤ In ≤ 5 Vdc (OFF state);
18 Vdc ≤ In ≤ 30 Vdc (ON state);

Description:

By means of SWC5090 Configuration Software, as user interface on PC to comunicate with the module, select Configuration table and impose Outputs configuration with "Hardware": Output 1 = Input 1 ; Output 2 = Input 2 ; Output 3 = Input 3. "Advanced Options" (found by clicking on the "Module > Advanced Options") has NOT been applied for this functional safety analysis, therefore "Advanced Options" must NOT be used for this application and Modbus communication must NOT be used for Functional Safety purpose.

The module is powered by connecting 24 Vdc power supply to Pins 9 (+ positive) - 10 (- negative). The green LED is lit in presence of supply power.

Input signals from Safety PLC can be applied to: Pins 1(+)-2(-) (In 1 - Ch.1), Pins 3(+)-4(-) (In 2 - Ch.2), Pins 5(+)-6(-) (In 3 - Ch.3). For each channel, a yellow LED is lit in presence of input signal (18 Vdc ≤ In ≤ 30 Vdc (ON state)). Only an input channel (1 or 2 or 3) and one of three (A or B or C) its outputs are Functional Safety related for a NE load.

Safety Function and Failure behavior:

D5240T is considered to be operating in Low Demand mode, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.

For each channel and each its output of D5240T module to drive a NE load, the failure behavior is described by the following definitions:

□ fail-Safe State: it is defined as each output (A and B and C) of used channel being de-energized;

□ fail Safe: failure mode that causes the module / (sub)system to go to the defined Fail-Safe state without a demand from the process;

□ fail Dangerous: a failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined Fail-Safe state), so that each output (A and B and C) of used channel remains energized;

□ fail Dangerous Detected: it's a dangerous failure which has been detected from D5240T internal diagnostic so that each output (A and B and C) of used channel is forced to de-energized state;

□ fail "No effect": failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure. When calculating the SFF this failure mode is not taken into account.

□ fail "Not part": failure mode of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account.

As the module has been evaluated in accordance with Route 2H (proven-in-use) of the IEC 61508:2010, Diagnostic Coverage DC ≥ 60% is required for Type B elements.

Being HFT = 0, in Low Demand mode the maximum achievable functional safety level is SIL 2.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	28.99
λ_{du} = Total Dangerous Undetected failures	18.79
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	211.25
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**259.03**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**440 years**
$\lambda_{no\ effect}$ = "No effect" failures	239.46
$\lambda_{not\ part}$ = "Not Part" failures	102.70
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**601.19**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**190 years**

Failure rates table according to IEC 61508:2010 Ed.2:

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	211.25 FIT	28.99 FIT	18.79 FIT	60.67%	92.75%

where DC means the diagnostic coverage by module internal diagnostic circuits.

This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 60.67 % ≥ 60 % as required by Route 2H evaluation (proven-in-use) of the IEC 61508:2010.

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes ≤10% of total SIF dangerous failures:

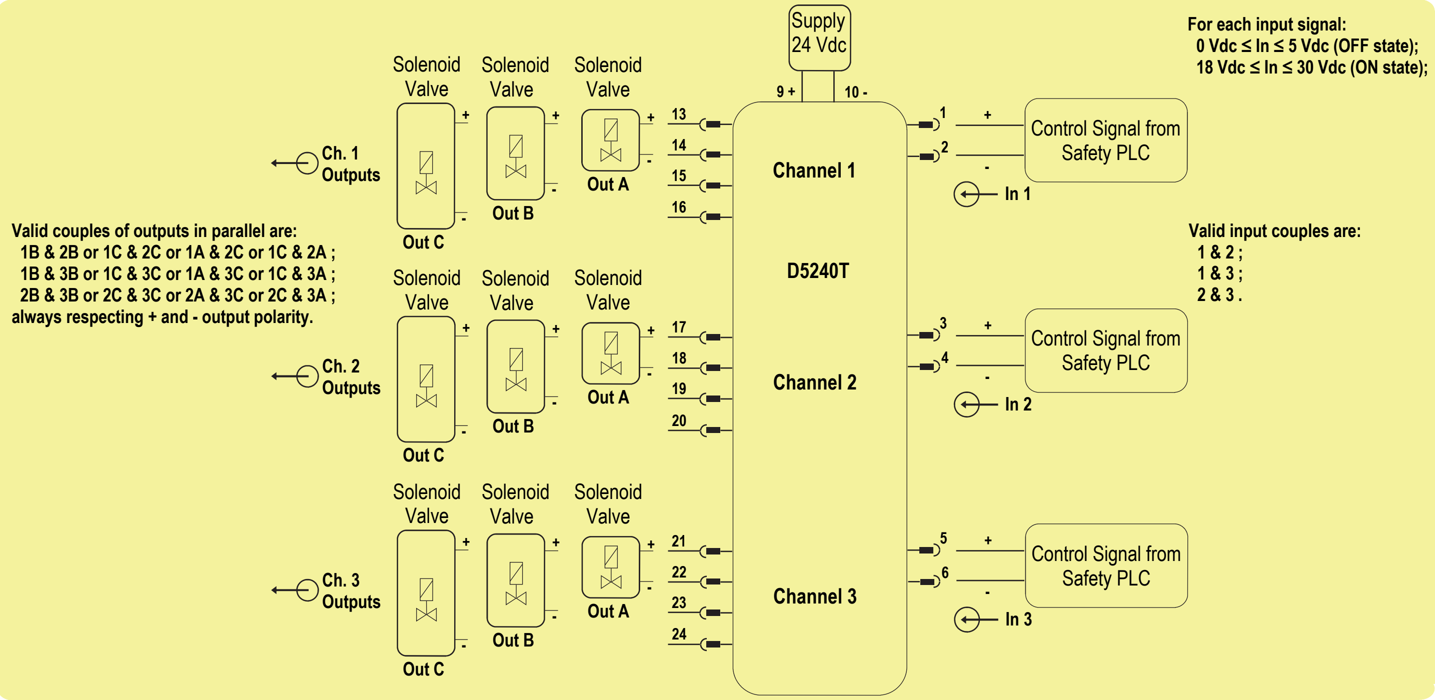
T[Proof] = 1 year	T[Proof] = 12 years
PFDavg = 8.27 E-05 Valid for **SIL 2**	PFDavg = 9.92 E-04 Valid for **SIL 2**

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

T[Proof] = 20 years
PFDavg = 1.65 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3.

2nd application of D5240T, with a couple of inputs (1 & 2 or 1 & 3 or 2 & 3) and related outputs in parallel (only B & B or C & C or A & C) for NE load


Supply
24 Vdc
9 +
10 -
For each input signal:
0 Vdc ≤ In ≤ 5 Vdc (OFF state);
18 Vdc ≤ In ≤ 30 Vdc (ON state);
Solenoid Valve
Solenoid Valve
Solenoid Valve
Ch. 1 Outputs
Out C
Out B
Out A
13
14
15
16
Channel 1
1
2
+
-
Control Signal from Safety PLC
In 1
Valid couples of outputs in parallel are:
1B & 2B or 1C & 2C or 1A & 2C or 1C & 2A ;
1B & 3B or 1C & 3C or 1A & 3C or 1C & 3A ;
2B & 3B or 2C & 3C or 2A & 3C or 2C & 3A ;
always respecting + and - output polarity.
D5240T
Valid input couples are:
1 & 2 ;
1 & 3 ;
2 & 3 .
Ch. 2 Outputs
17
18
19
20
Channel 2
3
4
In 2
Ch. 3 Outputs
21
22
23
24
Channel 3
5
6
In 3

Description:

By means of SWC5090 Configuration Software, as user interface on PC to comunicate with the module, select Configuration table and impose Outputs configuration with "Hardware": Output 1 = Input 1 ; Output 2 = Input 2 ; Output 3 = Input 3. "Advanced Options" (found by clicking on the "Module > Advanced Options") has NOT been applied for this functional safety analysis, therefore "Advanced Options" must NOT be used for this application and Modbus communication must NOT be used for Functional Safety purpose.

The module is powered by connecting 24 Vdc power supply to Pins 9 (+ positive) - 10 (- negative). The green LED is lit in presence of supply power. Input signals from Safety PLC can be applied to: Pins 1(+)-2(-) (In 1 - Ch.1), Pins 3(+)-4(-) (In 2 - Ch.2), Pins 5(+)-6(-) (In 3 - Ch.3). For each channel, a yellow LED is lit in presence of input signal (18 Vdc ≤ In In ≤ 30 Vdc (ON state)). Only a couple of inputs (1 & 2 or 1 & 3 or 2 & 3) and related outputs in parallel (only B & B or C & C or A & C) are Functional Safety related for a NE load.

Safety Function and Failure behavior:

D5240T is considered to be operating in Low Demand mode, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.

For each couple of channels and related outputs in parallel of D5240T module to drive a NE load, the failure behavior is described by the following definitions:

□ fail-Safe State: it is defined as one of two outputs in parallel or both outputs in parallel being de-energized;

□ fail Safe: failure mode that causes the module / (sub)system to go to the defined Fail-Safe state without a demand from the process;

□ fail Dangerous: a failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined Fail-Safe state), so that both outputs in parallel remain energized;

□ fail Dangerous Detected: it's a dangerous failure which has been detected from D5240T internal diagnostic so that each output (A and B and C) of each used channel is forced to de-energized state;

□ fail "No effect": failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure. When calculating the SFF this failure mode is not taken into account.

□ fail "Not part": failure mode of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account.

As the module has been evaluated in accordance with Route 2H (proven-in-use) of the IEC 61508:2010, Diagnostic Coverage DC ≥ 60% is required for Type B elements.

Being HFT = 0, in Low Demand mode the maximum achievable functional safety level is SIL 2.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	28.99
λ_{du} = Total Dangerous Undetected failures	12.48
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	226.33
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**267.80**
MTBF (safety function, two channels in parallel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**426 years**
$\lambda_{no\ effect}$ = "No effect" failures	263.29
$\lambda_{not\ part}$ = "Not Part" failures	70.10
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**601.19**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**190 years**

Failure rates table according to IEC 61508:2010 Ed.2:

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	226.33 FIT	28.99 FIT	12.48 FIT	69.91%	95.34%

where DC means the diagnostic coverage by module internal diagnostic circuits.

This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 69.91 % ≥ 60 % as required by Route 2H evaluation (proven-in-use) of the IEC 61508:2010.

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes ≤10% of total SIF dangerous failures:

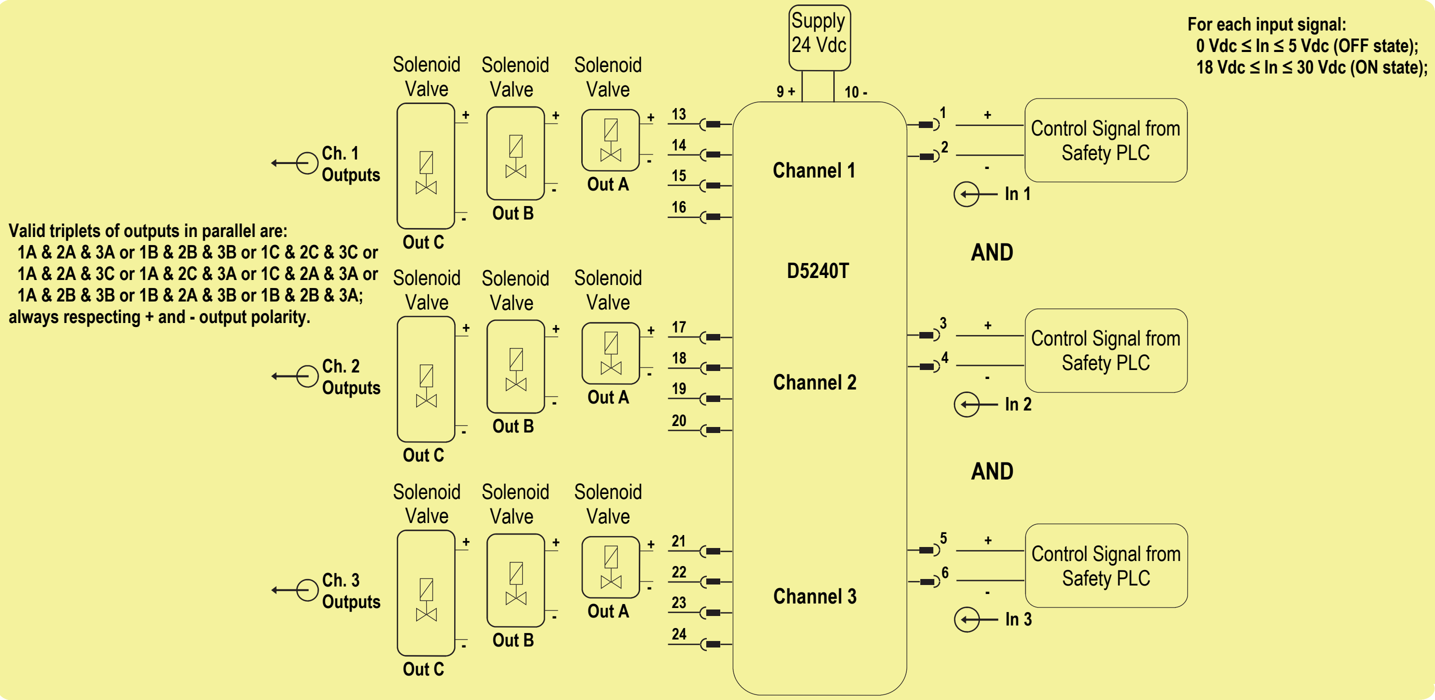
T[Proof] = 1 year	T[Proof] = 18 years
PFDavg = 5.50 E-05 Valid for **SIL 2**	PFDavg = 9.90 E-04 Valid for **SIL 2**

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

T[Proof] = 20 years
PFDavg = 1.10 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3.

3rd application of D5240T, with all inputs & related outputs in parallel (only A & A & A or B & B & B or C & C & C or A & A & C or A & B & B) for NE load



For each input signal:
0 Vdc ≤ In ≤ 5 Vdc (OFF state);
18 Vdc ≤ In ≤ 30 Vdc (ON state);

Valid triplets of outputs in parallel are:
1A & 2A & 3A or 1B & 2B & 3B or 1C & 2C & 3C or
1A & 2A & 3C or 1A & 2C & 3A or 1C & 2A & 3A or
1A & 2B & 3B or 1B & 2A & 3B or 1B & 2B & 3A;
always respecting + and - output polarity.

Description:

By means of SWC5090 Configuration Software, as user interface on PC to comunicate with the module, select Configuration table and impose Outputs configuration with "Hardware": Output 1 = Input 1 ; Output 2 = Input 2 ; Output 3 = Input 3. "Advanced Options" (found by clicking on the "Module > Advanced Options") has NOT been applied for this functional safety analysis, therefore "Advanced Options" must NOT be used for this application and Modbus communication must NOT be used for Functional Safety purpose.

The module is powered by connecting 24 Vdc power supply to Pins 9 (+ positive) - 10 (- negative). The green LED is lit in presence of supply power. Input signals from Safety PLC can be applied to: Pins 1(+)-2(-) (In 1 - Ch.1), Pins 3(+)-4(-) (In 2 - Ch.2), Pins 5(+)-6(-) (In 3 - Ch.3). For each channel, a yellow LED is lit in presence of input signal (18 Vdc ≤ In In ≤ 30 Vdc (ON state)). All inputs and related outputs in parallel (only A & A & A or B & B & B or C & C & C or A & A & C or A & B & B) are Functional Safety related for a NE load.

Safety Function and Failure behavior:

D5240T is considered to be operating in Low Demand mode, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.

For all channels and related outputs in parallel of D5240T module to drive a NE load, the failure behavior is described by the following definitions:

□ fail-Safe State: it is defined as one of three outputs in parallel or two of three outputs in parallel or all three outputs in parallel being de-energized;

□ fail Safe: failure mode that causes the module / (sub)system to go to the defined Fail-Safe state without a demand from the process;

□ fail Dangerous: a failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined Fail-Safe state), so that all three outputs in parallel remain energized;

□ fail Dangerous Detected: it's a dangerous failure which has been detected from D5240T internal diagnostic so that each output (A and B and C) of each channel is forced to de-energized state;

□ fail "No effect": failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure. When calculating the SFF this failure mode is not taken into account.

□ fail "Not part": failure mode of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account.

As the module has been evaluated in accordance with Route 2H (proven-in-use) of the IEC 61508:2010, Diagnostic Coverage DC ≥ 60% is required for Type B elements.

Being HFT = 0, in Low Demand mode the maximum achievable functional safety level is SIL 2.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	28.99
λ_{du} = Total Dangerous Undetected failures	13.43
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	241.41
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**283.83**
MTBF (safety function, three channels in parallel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**402 years**
$\lambda_{no\ effect}$ = "No effect" failures	279.86
$\lambda_{not\ part}$ = "Not Part" failures	37.50
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**601.19**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**190 years**

Failure rates table according to IEC 61508:2010 Ed.2:

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	241.41 FIT	28.99 FIT	13.43 FIT	68.34%	95.27%

where DC means the diagnostic coverage by module internal diagnostic circuits.

This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 68.34 % ≥ 60 % as required by Route 2H evaluation (proven-in-use) of the IEC 61508:2010.

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes ≤10% of total SIF dangerous failures:

T[Proof] = 1 year	T[Proof] = 16 years
PFDavg = 5.92 E-05 Valid for **SIL 2**	PFDavg = 9.47 E-04 Valid for **SIL 2**

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

T[Proof] = 20 years
PFDavg = 1.18 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3.

Testing procedure at T-proof

The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic.
This means that it is necessary to specify how dangerous undetected faults, which have been noted during the FMEDA, can be revealed during the proof test.

Proof test (to reveal approximately 99 % of possible Dangerous Undetected failures in the digital output module) consist of the following steps:

Steps	Action
1	Bypass the Safety PLC or take any other appropriate action to avoid a false trip.
2	The series connection of a 1 kΩ load resistor and an ammeter must be connected, in parallel with a voltmeter, to one of three outputs (first Out A, then Out B and finally Out C) for each of three channels (first Ch.1, then Ch.2 and finally Ch.3). Supply the D5240T module at 24 Vdc. Then, apply the control signal to each of three input channels (first In 1 of Ch.1, then In 2 of Ch.2 and finally In 3 of Ch.3), which can have the following two states: □ OFF = 0 Vdc ≤ In ≤ 5 Vdc, implying that the load current is 0 mA and the load voltage is 0 V because the 1 kΩ load resistor must be de-energized in accordance with the control input signal OFF state; □ ON = 18 Vdc ≤ In ≤ 30 Vdc, so that the 1 kΩ load resistor must be energized, with the following current and voltage values: - 19.5 ÷ 20.5 mA and 19.5 ÷ 20.5 V (for Out A); - 18.5 ÷ 19.5 mA and 18.5 ÷ 19.5 V (for Out B); - 18 ÷ 19 mA and 18 ÷ 19 V (for Out C).
3	Consider the configuration setup defined in the previous step (**2**) and replace the series connection of a 1 kΩ load resistor and an ammeter with a current calibrator (set to 30 mA). This current generator and a voltmeter are connected in parallel to one of three outputs (first Out A, then Out B and finally Out C) for each of three channels (first Ch.1, then Ch.2 and finally Ch.3). Supply the D5240T module at 24 Vdc and apply a 24 Vdc (ON state) control signal to each of three input channels (first In 1 of Ch.1, then In 2 of Ch.2 and finally In 3 of Ch.3), verifying the following load voltage values: 18.0 ÷ 18.5 V (for Out A), 16.0 ÷ 16.5 V (for Out B) and 15.0 ÷ 15.5 V (for Out C).
4	Restore the loop to full operation.
5	Remove the bypass from the Safety PLC or restore normal operation.